The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/08/2010

SUBJECT:
Multiple Vulnerabilities in Apple QuickTime Player Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple QuickTime Player that could allow remote code execution. Apple QuickTime Player is used to play media files on Microsoft Windows and Mac OS X operating systems. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of Apple QuickTime Player. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Apple QuickTime 7.6.8 and earlier

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Apple QuickTime Player that could allow remote code execution. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of Apple QuickTime Player.

The following vulnerabilities have been identified by Apple:
- Two heap buffer overflow vulnerabilities affecting Apple QuickTime exists when opening either a specially crafted JP2 image or a movie file that contains specially crafted 'Track Header' (tkhd) atoms.

- Four memory corruption vulnerabilities affecting Apple QuickTime exist when handling specially crafted PICT files, QTVR files, FlashPix images, and Sorenson encoded movie files.
- An Integer Overflow vulnerability affecting Apple QuickTime exists when handling a specially crafted movie file.
- A local information disclosure vulnerability affecting Apple QuickTime exists due to a filesystem permission issue. A local attacker could exploit this issue to obtain sensitive information that may aid in further attacks.
- Threeuninitialized memory access issues exists in QuickTime's handling of JP2, FlashPix, and GIF images.
- Two memory corruption issues affect QuickTime's handling of avi and movie files
- A buffer overflow vulnerability exists in QuickTime's handling of MPEG encoded movie files
- A signedness issue exists in QuickTime's handling of MPEG encoded movie files.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts withfull user rights. Failed attempts could result in a denial-of-service.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Apple:
http://www.apple.com/quicktime/download/

http://lists.apple.com/archives/security-announce/2010/Dec/msg00000.html

http://support.apple.com/kb/HT4447

Security Focus:
http://www.securityfocus.com/advisories/21050

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4009

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0530

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3801

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3802

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1508

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3800

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3787

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3788

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3789

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3790

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3791

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3792

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3793

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3794

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3795